

DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of the Army organizational name (APMS Sub Organization name).

Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command (F&MWRC)

2. Name of Information Technology (IT) System (APMS System name).

Virtual Army Community Services (VACS)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

590

5. IT Investment (OMB Circular A-1 1) Unique Identifier (if applicable)

NA

6. Privacy Act System of Records Notice Identifier (if applicable).

A0215 CFSC, General Morale, Welfare, Recreation and Entertainment Records
(October 17, 2001, 66 FR 52750)

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

NA

8. Type of authority to collect information (statutory or otherwise).

5 USC 3111 Volunteer Documentation;
10 USC 1588, Volunteer Services;
10 U.S.C. 3013, Secretary of the Army;
26 U.S.C. 6041, Information at Source;
Army Regulation 215-1 Morale Welfare, and Recreation Activities and Non-appropriated Fund Instrumentalities;
Army Regulation 608-1 ACS Policy & Family and Soldier Readiness System;
DoD Directive 1015.2, Military Morale, Welfare and Recreation (MWR);
DoD Instruction 1015.10, Program for Military Morale, Welfare, and Recreation (MWR);
Executive Order 12072

E.O. 9397 (SSN)

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries, and interconnections, location of system and components, and system backup).

Virtual Army Community Services is the online face of the Family Program (FP) Directorate, at Headquarters Department of the Army (HQDA) to FP personnel. FP has an on-going requirement to train and convey in a timely manner new and accurate information to family members of the Army, to include active, guard and reserve components geographically dispersed world wide. To meet this geographical challenge and to fulfill the purpose, the web-based system was determined to possess the best combination of accessibility, deployment and cost for meeting the aforementioned needs. This system is currently in use and in its second year of development. It is owned by HQDA Family Programs Directorate and operated by DefenseWeb Technologies, Inc. The various components of the web system are the Army Community Services The ACS Management Report System and the Client Tracking System are parts of VACS. All systems are backed up on a nightly and weekly schedule.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

The personally identifiable information (PII) collected for ACS personnel includes name, e-mail address, military community, position title, work phone and fax numbers. The personally identifiable information collected for clients includes name, gender, rank, social security or alien registration number, and birth date. The source of ACS personnel information is directly from the staff member; the source of client information is directly from the individual client to ACS personnel who enter it into the system. The system is accessed by an username and password and mailing a

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

ACS personnel information is entered by the individual staff member and then verified by their managers. Client information is entered by ACS personnel from face-to-face personal interview.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

PII is collected to establish an individual's identity and eligibility for ACS Services and to verify that ACS personnel should have access to the system.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

Initially, PII is used to establish an individual's identity and later to verify an individual's identity against data on file to establish routine user sessions; to evaluate individuals who apply for volunteer services; to register conference attendees and conduct background security checks; to account for and provide training to spouses. Data is also used to assess manpower trends and patterns, to determine historical, current and future trends and needs, as well as to produce statistical studies and reports required by Assistant Secretary of Defense for Force Management and Personnel.

14. Describe whether the system derives or creates new data about individuals through aggregation.

This system does not create new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

The information may be viewed by internal developers, system administrators, ACS managers and staff, as well as individuals, who can view their own information in the system. No other system or component interfaces with VACS.

Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

A link to a privacy web page is displayed on the website's home page and on the registration page. The Privacy Act is to be read by the ACS Staff member to the client. At that time, a client may object to the collection of personal information. No client information can be recorded until a checkbox has been checked by the Staff member acknowledging that they have spoken with the client about the privacy act information.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

Before intake of a client's record, a Privacy Act Statement is displayed giving a section on authority, principal purpose, routine uses, and disclosure for the system. The Privacy Act is to be read by the ACS Staff member to the client. No client information can be recorded until a checkbox has been checked by the Staff member acknowledging that they have spoken with the client about the privacy act information.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

This government computer system employs software programs to monitor network traffic, to identify unauthorized attempts to upload or change information, to cause damage, or to deny service to authorized users. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

All ACS personnel accessing government computer information are required to receive, at a minimum, favorable local, state and national security checks. The users include Federal Civil Service personnel and authorized contractors of ACS that have a need to know in order to perform official government duties. Both contractor and government employees may have access requirements and are limited to specific or general information in the computing environment; therefore, certain types of data are restricted to only certain access levels within the system. Each user has a unique username and password for the system. If the user has an access level to retrieve data, their username and password will allow them to view it. These access levels are assigned by system administrators to authorized personnel as needed. Data search results in the system are for one record, as opposed to searching through multiple data records. All data is filtered by installations and can not be searched by users not authorized for the particular installation for which the data is stored. This system has a current certification and accreditation. The system resides on secure military installations within secured facilities.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A systems notice currently exists and either it will be amended to be more descriptive of this business practice, or an entirely new system notice will be developed.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying

individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only. The PIA may be published in full.